線型符号に対する新たなMac Williams型恒等式(代数的組合せ論)

AUTHOR(S):

城本, 啓介

CITATION:

城本, 啓介. 線型符号に対する新たなMac Williams型恒等式(代数的組合せ論). 数理解析研究所講究録 1996, 962: 128-132

ISSUE DATE:

1996-08

URL:

http://hdl.handle.net/2433/60536

数理解析研究所講究録
962巻 1996年 128-132

線型符号に対する新たなMac Williams 型恒等式

熊本大・理　城本啓介（keisuke Shiromoto）

線型符号で用いられる簡単な記号をまず定義する。

$F := \mathbb{F}_q$　　(q-elements field)

$V := F^n := \{(u_1, \cdots, u_n) \mid u_i \in F\}$

$N := \{1, 2, \cdots, n\}$

$\forall u = (u_1, \cdots, u_n), v = (v_1, \cdots, v_n) \in V$ に対して.

$\langle u, v \rangle := \sum_{i=1}^{n} u_i v_i$

$d(u, v) := \#\{i \in N \mid u_i \neq v_i\}$

$\mathrm{supp}(u) := \{i \in N \mid u_i \neq 0\}$

$|u| = W_t(u) := |\mathrm{supp}(u)|$ 。

Definition

(1) C : (lenear) code $\rightleftarrows$ $C \leq V$ (subspace)

特に、$\dim C = k$ のとき、$C : [n, k]$-code という。

（ここで、$n = \dim V =$ length of C ）

(2) $C^\perp$: dual code of C

$\rightleftarrows$ $C^\perp := \{v \in V \mid \langle u, v \rangle = 0, \forall u \in C\}$

次に、codeとそのdual codeの関係を恒等式により、考察すると、次の有名な2つの定理がある。

Definition

$W_C(x,y)$: Weight enumerator of C

$\rightleftarrows$ $W_C(x,y) := \sum_{u \in C} x^{n-|u|} y^{|u|} = \sum_{r=0}^{n} a_r x^{n-r} y^r$

(ここで、x, y：変数，$a_r := \#\{u \in C \mid |u| = r\}$)

Theorem 1 (MacWilliams (1963))

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+(q-1)y,\ x-y)$$

Definition

$W_{C,D}(a,b,c,d)$: Joint weight enumerator of C and D

$\rightleftarrows$ $W_{C,D}(a,b,c,d) := \sum_{u \in C} \sum_{v \in D} a^{i(u,v)} b^{j(u,v)} c^{k(u,v)} d^{l(u,v)}$

(ここで、a, b, c, d：変数，

$i(u,v) := \#\{i \in N \mid u_i = 0,\ v_i = 0\}$,

$j(u,v) := \#\{i \in N \mid u_i = 0,\ v_i \neq 0\}$,

$k(u,v) := \#\{i \in N \mid u_i \neq 0,\ v_i = 0\}$,

$l(u,v) := \#\{i \in N \mid u_i \neq 0,\ v_i \neq 0\}$.)

Theorem 2 (MacWilliams, Mallows, Sloane (1972))

$$W_{C^\perp,D^\perp}(a,b,c,d)=\frac{1}{|C|\cdot|D|}W_{C,D}(a+\gamma(b+c)+\gamma^2 d,\ a-b+\gamma(c-d),$$

$$a-c+\gamma(b-d),\ a-b-c+d)$$

(ここで、$\gamma=\delta-1$)

以上、2つの定理では1つまたは2つのベクトルのWeightについて考えてあるが、これをλ個のベクトルに拡張することにより、次の定理が得られる。

Definition $\forall\lambda\in\mathbb{N}$ に対して、

$$W_C^{(\lambda)}(x,y):=\sum_{u^{(1)},\cdots,u^{(\lambda)}\in C} x^{n-s(u^{(1)},\cdots,u^{(\lambda)})}\,y^{s(u^{(1)},\cdots,u^{(\lambda)})}$$

(ここで、$s(u^{(1)},\cdots,u^{(\lambda)}):=\#\{i\in N\mid u_i^{(j)}\neq 0,\ \exists j\in\{1,2,\cdots,\lambda\}\}$

$=|\mathrm{supp}(u^{(1)})\cup\cdots\cup\mathrm{supp}(u^{(\lambda)})|$)

Theorem 3 (Shiromoto (1995))

$$W_{C^\perp}^{(\lambda)}(x,y)=\frac{1}{|C|^\lambda}W_C^{(\lambda)}(x+(\delta^\lambda-1)y,\ x-y)$$

Remarks (1) $\lambda=1$ とすることにより、$W_C^{(1)}(x,y)=W_C(x,y)$ となり、Th1の恒等式と一致する。

(2) $\lambda=2$ とすることにより、$W_C^{(2)}(x,y)=W_{C,C}(x,y,y,y)$ とな

1)、Th2の恒等式と一致する。

つまり、Th3は、Th1, Th2の拡張になっている。

Example H_3 : binary Hamming code of length 3

$H_3 = \{000, 110, 101, 011\}$, $H_3^{\perp} = \{000, 111\}$ より

$W_{H_3}^{(\lambda)}(x,y) = x^3 + 3(2^\lambda - 1)xy^2 + (4^\lambda - 3\cdot 2^\lambda + 2)y^3$

$W_{H_3^{\perp}}^{(\lambda)}(x,y) = x^3 + (2^\lambda - 1)y^3$

ここで、$\frac{1}{|H_3|^\lambda} W_{H_3}^{(\lambda)}(x+(2^\lambda-1)y, x-y)$

$= \cdots = x^3 + (2^\lambda - 1)y^3$ となり

$W_{H_3^{\perp}}^{(\lambda)}(x,y) = \frac{1}{|H_3|^\lambda} W_{H_3}^{(\lambda)}(x+(2^\lambda-1)y, x-y)$ が成立する。

(Theorem 3 の証明の概略)

$D \leq V$, $R \subseteq N$ に対して、

$D(R) := \{u \in D \mid \mathrm{supp}(u) \subseteq R\}$

$D^* := \mathrm{Hom}_F(D, F) \cong V/D^{\perp}$ とおくと

$$0 \longrightarrow C^{\perp}(R) \xrightarrow{\mathrm{inc}} V(R) \xrightarrow{f} C^* \xrightarrow{\mathrm{res}} C(N-R)^* \longrightarrow 0$$

: exact (Tomoyuki Yoshida) となる。

ここで、$f : v \longmapsto (\hat{v} : u \longmapsto \langle u, v \rangle)$

$$\therefore\ |C|\cdot|C^{\perp}(R)| = |V(R)|\cdot|C(N-R)| \quad \text{——①}$$

さらに、$\widetilde{W}_C^{(\lambda)}(x,y) := \sum_{R\subseteq N} |C(R)|^{\lambda} x^{n-|R|} y^{|R|}$ $(\forall \lambda \in \mathbb{R})$ とおくと、

$$\widetilde{W}_{C^{\perp}}^{(\lambda)}(x,y) = \frac{1}{|C|^{\lambda}} \sum_{R\subseteq N} |V(R)|^{\lambda}\cdot|C(N-R)|^{\lambda} x^{n-|R|} y^{|R|} \quad (\because ①)$$

$$= \frac{1}{|C|^{\lambda}} \widetilde{W}_C^{(\lambda)}(q^{\lambda}y, x)$$

また、二項定理を用いると、$\widetilde{W}_C^{(\lambda)}(x,y) = W_C^{(\lambda)}(x+y, y)$

$$\therefore\ W_{C^{\perp}}^{(\lambda)}(x,y) = \widetilde{W}_{C^{\perp}}^{(\lambda)}(x-y, y)$$

$$= \frac{1}{|C|^{\lambda}} W_C^{(\lambda)}(q^{\lambda}y, x-y)$$

$$= \frac{1}{|C|^{\lambda}} W_C^{(\lambda)}(x+(q^{\lambda}-1)y, x-y) \ //$$

次に、証明の所で定義した $\widetilde{W}_C^{(\lambda)}(x,y)$ について、両辺を λ で微分し、$\lambda = 0$ を代入すると、次のようになる。

$$\left.\frac{\partial}{\partial \lambda}\widetilde{W}_C^{(\lambda)}(x,y)\right|_{\lambda=0} = \frac{1}{\log_q e} \sum_{R\subseteq N} \dim C(R)\, x^{n-|R|} y^{|R|}$$

ここで、$W_C^{\dim}(x,y) := \sum_{R\subseteq N} \dim C(R)\, x^{n-|R|} y^{|R|}$ とおくと、

<u>Theorem 4</u> (T. Yoshida, Shiromoto (1995))

$$W_{C^{\perp}}^{\dim}(x,y) = (x+y)^{n-1}\{(n-k)y - kx\} + W_C^{\dim}(y,x)$$